CLAIMS

What is claimed is:

1. A server that provides services to clients connected to the server via a network, the server comprising:

a public-key storage unit for storing public keys assigned to each service provided by the server;

a challenge generator for generating a challenge to be sent from the server to the client after the server receives a request for a service from the client;

an access privilege verifier for verifying, using a corresponding public key, whether a prescribed relationship exists between the challenge transmitted to the client and a response to that challenge received from the client; and

a controlling unit, while authenticating access privilege of the client for a service provided by the server,

for transmitting the challenge generated by the challenge generator to the client;

for receiving the response to that challenge returned from the client;

for verifying, with an access privilege verifier using a public key assigned to the service and stored in the public-key storage unit, whether a prescribed relationship exists between the challenge and the response; and

for providing the service to the client only when the access privilege verifier successfully verifies the relationship.

2. A client that requests services from a server connected to the client via a network, the client comprising:

auniqueoperationexecutorforexecutingauniqueoperation assigned to the client;

an access privilege proving data storage unit for storing access privilege proving data created from a private key corresponding to a public key assigned to the requested service and the result of the unique operation;

aresponsegeneratorforgeneratingaresponsetoachallenge received from the server by executing a prescribed calculation using the result of the unique operation and the access privilege proving data; and

a controlling unit, while proving to the server that the client owns the access privilege for the service provided by the server,

for receiving the challenge from the server;

for generating, with the response generator, the response from (a) the challenge, (b) the result of the uniqueoperationexecutedbytheuniqueoperationexecutor, and (c) the access privilege proving data stored in the

access privilege proving data storage unit; and

for transmitting the created response to the server.

3. A client that requests services from a server connected to the client via a network, comprising:

a portable device connector for connecting to a portable device provided with a unique operation generator for executing unique operations;

an access privilege proving data storage unit for storing access privilege proving data created from a private key corresponding to a public key assigned to the requested service and the result of the unique operation assigned to the portable device;

a response generator for generating a response to a challenge received from the server by executing a prescribed calculation using the result of the unique operation and the access privilege proving data; and

a controlling unit, while proving to the server that the client owns the access privilege for the service provided by the server,

for receiving the challenge from the server;

for generating, with the response generator, the response from (a) the challenge, (b) the result of the unique operation executed by the unique operation executor

housed in the portable device connected to the portable device connector, and (c) the access privilege proving data stored in the access privilege proving data storage unit; and

for transmitting the created response to the server.

4. A server that provides services to clients connected to the server via a network, the server comprising:

a public-key storage unit for storing public keys assigned to each service provided by the server;

a challenge generator for generating a challenge to be sent from the server to the client after the server receives a request for a service from the client;

an access privilege verifier for verifying, using a corresponding public key, whether a prescribed relationship exists among the challenge transmitted to the client, a response to that challenge received from the client, and an access privilege proving data for proving the access privilege of the client; and

a controlling unit, while authenticating access privilege of the client for a service provided by the server,

for transmitting the challenge generated by the challenge generator to the client;

for receiving the response to that challenge returned

from the client, and ;

for verifying, with an access privilege verifier using a public key assigned to the service and stored in the public-key storage unit, whether a prescribed relationship exists among the challenge, the access privilege proving data for proving the access privilege of the client for the service, and the response; and

for providing the service to the client only when the access privilege verifier successfully verifies the relationship.

5. A client that requests services from a server connected to the client via a network, the client comprising:

auniqueoperationexecutorforexecutingauniqueoperation assigned to the client;

an access privilege proving data storage unit for storing access privilege proving data created from a private key corresponding to a public key assigned to the requested service and the result of the unique operation;

aresponsegeneratorforgeneratingaresponsetoachallenge received from the server by executing a prescribed calculation using the result of the unique operation; and

a controlling unit, while proving to the server that the client owns the access privilege for the service provided by

the server,

for receiving the challenge from the server;

for generating, with the response generator, the response from (a) the challenge, and (b) the result of the unique operation executed by the unique operation executor; and

for transmitting to the server, the created response, and the access privilege proving data stored in the access privilege proving data storage unit.

6. A client that requests services from a server connected to the client via a network, comprising:

a portable device connector for connecting to a portable device provided with a unique operation generator for executing unique operations;

an access privilege proving data storage unit for storing access privilege proving data created from a private key corresponding to a public key assigned to the requested service and the result of the unique operation assigned to the portable device;

a response generator for generating a response to a challenge received from the server by executing a prescribed calculation using the result of the unique operation; and

a controlling unit, while proving to the server that the

client owns the access privilege for the service provided by the server,

for receiving the challenge from the server;

for generating, with the response generator, the response from (a) the challenge, and (b) the result of the unique operation executed by the unique operation executor housed in the portable device connected to the portable device connector; and

for transmitting to the server, the created response, and the access privilege proving data stored in the access privilege proving data storage unit.

7. A client as recited in claim 3, wherein the access privilege proving data storage unit is included in the portable device connected to the portable device connector.

8. A client as recited in claim 6, wherein the access privilege proving data storage unit is included in the portable device connected to the portable device connector.

9. A server as recited in claim 1, wherein the server is a web server that supplies web applications to clients; and the public keys stored in the public-key storage unit are assigned to individual web pages provided to the clients and are used

to verify the access privileges of the client for a web page when the server receives a request from the client to access a web page.

10. A server as recited in claim 4, wherein the server is a web server that supplies web applications to clients; and the public keys stored in the public-key storage unit are assigned to individual web pages provided to the clients and are used to verify the access privileges of the client for a web page when the server receives a request from the client to access a web page.

11. A server as recited in claim 1, wherein the server is a web server that supplies web applications to clients; and the public keys stored in the public-key storage unit are assigned to groups of web pages provided to the clients and are used to verify the access privileges of the client for a web page when the server receives a request from the client to access a web page in one of the groups of web pages.

12. A server as recited in claim 4, wherein the server is a web server that supplies web applications to clients; and the public keys stored in the public-key storage unit are assigned to groups of web pages provided to the clients and are used

to verify the access privileges of the client for a web page when the server receives a request from the client to access a web page in one of the groups of web pages.

13. A server that provides services to clients connected to the server via a network, the server comprising:

a script interpreter for interpreting script designed to control the contents of services that the server provides to clients and for controlling the operations of the server; and

a privilege authenticator for authenticating access privileges of the client when called by the script interpreter.

14. A server as recited in claim 13, wherein the privilege authenticator comprises:

a challenge generator for generating a challenge to be sent from the server to the client; and

an access privilege verifier that uses a public key to verify a prescribed relationship between the challenge transmitted to the client and a response to that challenge returned from the client;

and the privilege authenticator receives a public key for authenticating privileges of the client when called by the script interpreter, transmits the challenge generated by the

challenge generator to the client, receives a response to the challenge sent by the client, and verifies, using the received public key, access privileges of the client by means of the access privilege verifier.

15. A server as recited in claim 13, wherein the privilege authenticator comprises:

a challenge generator for generating a challenge to be sent from the server to the client; and

an access privilege verifier that uses a public key to verify a prescribed relationship among the challenge transmitted to the client, a response to that challenge returned from the client, and access privilege proving data for verifying access privileges of the client;

and the privilege authenticator receives a public key for authenticating privileges of the client when called by the script interpreter, transmits the challenge generated by the challenge generator to the client, receives a response to the challenge sent by the client, and verifies, using the received public key, access privileges of the client by means of the access privilege verifier.

16. A method executed in a server for providing services from the server to clients connected to the server via a network

after verifying the access privileges of the clients for the services, public keys being assigned in advance to respective services provided by the server, the method comprising the steps of:

generating a challenge when a request for a service is received from a client and transmitting the challenge to the client;

receiving a response to the challenge returned from the client;

verifying that a prescribed relationship exists between the challenge sent to the client and the response received from the client using the public key assigned to the requested service; and

providing the requested service to the client only when the prescribed relationship exists.

17. A method executed in a client for proving its access privilege for a server when requesting a service from a server connected to the client via a network, the client being in advance assigned with a unique operation, the requested service being in advance assigned with a public key, the client in advance receiving access privilege proving data for expressing the access privilege of the client for the service, the access privilege proving data being created from a private key corresponding

to a public key assigned to the service and the result of a unique operation assigned to the client, the method comprising the steps of:

receiving a challenge from the server;

executing the unique operation assigned thereto;

generating a response based on the challenge received from the server, the result of the unique operation, and the access privilege proving data; and

transmitting the response to the server.

18. A method executed in a server for providing services from the server to clients connected to the server via a network after verifying the access privileges of the clients for the services, public keys being assigned in advance to respective services provided by the server, the method comprising the steps of:

generating a challenge when a request for a service is received from a client and transmitting the challenge to the client;

receiving a response to the challenge from the client;

verifying that a prescribed relationship exists among the challenge sent to the client, the response received from the client, and the access privilege proving data indicative of access privilege of the client for the service, using the

public key assigned to the requested service; and

providing the requested service to the client only when the prescribed relationship exists.

19. A method executed in a client for proving its access privilege for a server when requesting a service from a server connected to the client via a network, the client being in advance assigned with a unique operation, the requested service being in advance assigned with a public key, the client in advance receiving access privilege proving data for expressing the access privilege of the client for the service, the access privilege proving data being created from a private key corresponding to a public key assigned to the service and the result of a unique operation assigned to the client , the method comprising the steps of:

receiving a challenge from the server;

executing the unique operation assigned thereto;

generating a response based on the challenge received from the server, and the result of the unique operation; and

transmitting the response, and the access privilege proving data, to the server.

20. A client that requests services from a server connected to the client via a network, the client comprising:

auniqueoperationexecutorforexecutingauniqueoperation assigned to the client;

aresponsegeneratorforgeneratingaresponsetoachallenge received from the server by executing a prescribed calculation using the result of the unique operation; and

a controlling unit, while proving to the server that the client owns the access privilege for the service provided by the server,

for receiving the challenge from the server;

for generating, with the response generator, the response from (a) the challenge, and (b) the result of the unique operation executed by the unique operation executor; and

fortransmittingthecreatedresponsetotheserver.

21. A client that requests services from a server connected to the client via a network, comprising:

a portable device connector for connecting to a portable device provided with a unique operation generator for executing unique operations;

aresponsegeneratorforgeneratingaresponsetoachallenge received from the server by executing a prescribed calculation using the result of the unique operation; and

a controlling unit, while proving to the server that the

client owns the access privilege for the service provided by the server,

for receiving the challenge from the server;

for generating, with the response generator, the response from (a) the challenge, and (b) the result of the unique operation executed by the unique operation executor housed in the portable device connected to the portable device connector; and

for transmitting the created response to the server.